APPENDIX A

1. (Currently Amended) A method for setting basic means of access for operation of devices of which the operation is controllable by electronic means, comprising: said devices comprising mobile phones, small computer-controlled consumer devices with relatively low level of computing power, computers, motor vehicles, control terminals for industrial processes, all of which devices may require authentication prior to operation, said authentication comprising a temporary deactivation which adds authorization patterns of progressive hierarchies of access rights to said devices prior to said operation ;

establishment of a non split-key link between a personal authentication system supplied with encryption data and a logic system able to control an electronic device control, said encryption data being stored solely in said authentication system;

checking said encryption data in said authentication system prior to operation of said electronic device control;

assignment of a plurality of predetermined means of access to said electronic device control associated with said authentication system, said predetermined means providing access to physical hardware resources and access to different software functions, based on the privileges of the user who identified himself to the system, said software function evaluates a security token and is running on top of said physical hardware,

said predetermined means of access being dependent upon the level of authorization that is set in said personal authorization system; enabling of said predetermined means for access for said authentication system dependent on the result of said check;

<u>said method providing means for protecting said devices against unauthorized by rendering said devices configurable in a user friendly and secure way making them accessible for an individual, customized use by a person</u>.

2. (Previously presented) The method defined in Claim 1, wherein said basic means of access to functions of said device comprise at least one of the following means: disable operation of said devices, enable operation of said devices, or enable configuration of said devices.

3.(Previously presented) The method defined in Claim 2 wherein said link is made without need for intermediate software layers.

4. (Previously presented) The method defined in Claim 3 includes in addition, the step of reading at least one of the following features embodied within said authentication system: firmware programs, device-specific command sequences for execution of specific device-specific functions, cryptographic keys, cryptographic algorithms, and individual decision-making logic.

5.(Previously presented) The method defined in claim 4 which includes configuration of said devices; by authorized persons, wherein after successful authentication, device-specific configuration data are downloaded into said devices from said authentication system in accordance with said authentication systems or over a network.

6. (Previously presented) A device comprising the elements defined in Claim 5 for execution setting basic means of access for operations.

7. (Previously presented) An authentication system, created for authentication of a person or a group of people, comprising the elements defined in Claim 5.

8.(Previously presented) The authentication system defined in Claim 7 which is implemented in the form of a Smartcard .

9.(Previously presented) A system for setting basic means of access for operation of devices of which the operation is controllable by electronic means, including at least one device and an authentication system as defined in Claim 8.

10.(Previously presented) A computer program, containing program code areas for the execution or preparation for execution of the steps of the method in accordance with Claim 4, when said program is installed in a computer.

11. (Currently Amended) A method for setting basic means of access for operation of devices of which the operation is controllable by electronic means, comprising: said devices comprising small computer-controlled consumer devices with relatively low level of computing power, computers, motor vehicles, control terminals for industrial processes, all of which devices may require authentication prior to operation said authentication comprising temporary deactivation which adds authorization patterns of progressive hierarchies of access rights to said devices prior to said operation; establishment of a non split-key link between a personal authentication system supplied with encryption data and a logic system able to control an electronic device control, said encryption data being stored solely in said authentication system; checking said encryption data in said authentication system prior to operation of said electronic device control;

assignment of a plurality of predetermined means of access to said electronic device control associated with said authentication system; said predetermined means providing access to physical hardware resources and access to

different software functions, based on the privileges of the user who identified himself to the system, said software function evaluates a security token and is running on top of said physical hardware, said predetermined means of access being dependent upon the level of authorization that is set in said personal authorization system;

enabling of said means for access predetermined for said authentication system dependent on the result of said check;

said method providing means for protecting said devices against unauthorized by rendering said devices configurable in a user friendly and secure way making them accessible for an individual, customized use by a person.

12 (New) A method comprising: setting basic electronic means of access for operation of devices, said basic electronic means selected from the group consisting of disable operation of said devices, enable operation of said devices, and enable configuration of said devices; said operation being controllable by electronic means, said devices comprising mobile phones, small computer-controlled consumer devices with relatively low level of computing power, computers, motor vehicles, control terminals for industrial processes, all of which devices may require authentication prior to operation, said authentication comprising a temporary deactivation which adds authorization patterns of progressive hierarchies of access rights to said devices prior to said operation ;

establishment of a non split-key link between a personal authentication system comprising a Smartcard supplied with encryption data and a logic system able to control an electronic device control, said link being made without need for intermediate software layers; and said encryption data being stored solely in said authentication system;

reading at least one of the following features embodied within said authentication system: firmware programs, device-specific command sequences for execution of specific device-specific functions, cryptographic keys, cryptographic algorithms, and individual decision-making logic; and

checking said encryption data in said authentication system prior to operation of said electronic device control;

configuring said devices by authorized persons, wherein after successful authentication, device-specific configuration data are downloaded into said devices from said authentication system in accordance with said authentication systems or over a network

assignment of a plurality of predetermined means of access to said electronic device control associated with said authentication system, said predetermined means providing access to physical hardware resources and access to different software functions, based on the privileges of the user who identified himself to the system, said software function evaluates a security token and is running on top of said physical hardware,

said predetermined means of access being dependent upon the level of authorization that is set in said personal authorization system; enabling of said predetermined means for access for said authentication system dependent on the result of said check;

said method providing means for protecting said devices against unauthorized by rendering said devices configurable in a user friendly and secure way making them accessible for an individual, customized use by a person.

wherein said basic means of access to functions of said device comprise at least one of the following means: disable operation of said devices, enable operation of said devices, or enable configuration of said devices.

13. (New) A device comprising the elements defined in Claim 12 for execution setting basic means of access for operations.

14. (New) An authentication system, created for authentication of a person or a group of people, comprising the elements defined in Claim 12.

15. (New) A computer program, containing program code areas for the execution or preparation for execution of the steps of the method in accordance with Claim 12, when said program is installed in a computer.